Calhoun: The NPS Institutional Archive

Theses and Dissertations | Thesis Collection

2014-09

Resilient and fractionated cyber physical system

Connett, Brian

Monterey, California: Naval Postgraduate School

http://hdl.handle.net/10945/43894

http://www.nps.edu/library

Calhoun is a project of the Dudley Knox Library at NPS, furthering the precepts and goals of open government and government transparency. All information contained herein has been approved for release by the NPS Public Affairs Officer.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

RESILIENT AND FRACTIONATED CYBER PHYSICAL SYSTEM

by

Brian Connett

September 2014

Thesis Advisor: Alex Bordetsky
Second Reader: Daniel W. Bursch

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2014	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE
RESILIENT AND FRACTIONATED CYBER PHYSICAL SYSTEM

5. FUNDING NUMBERS

6. AUTHOR(S) Brian Connett

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

Reliance on aging monolithic overhead physical systems with assurance of resilience is an ongoing critical discussion. The White House has issued a strategy to evolve this system of systems technology to meet growing information and knowledge needs.

Fractionated Space Cyber Physical Systems is part of a novel concept emerging from a field of hyperconnected networks designed to withstand risk and address aforementioned needs. The transition from a monolithic design into alternative resilient designs will better reflect the utility of a system to the commander. Resilience is a characteristic meant to assure performance even within a higher probability of risk. Resilience encourages availability regardless of the perceived threat in the increasingly dynamic environment.

Traditional systems incorporate the sub-systems required to deliver the common operational picture. Reduction of those integrated sub-systems is unacceptable; therefore, introducing a decentralized architecture is going to carry with it the requirement of a seamless interaction despite being separated. Decentralization is a design process that allows a constellation capability to seek more nodes than what would be normally available when residing in the same payload. This is a measure of design success that enhances the evaluation of a system's capability and its ability to survive risk, its resilience.

14. SUBJECT TERMS Cyber Physical System, Fractionation, Space Based Group, Resilient, Resilience, Resiliency, Control Systems, System of Systems, Mobile Ad Hoc Network

15. NUMBER OF PAGES 55

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

RESILIENT AND FRACTIONATED CYBER PHYSICAL SYSTEM

Brian Connett
Lieutenant Commander, United States Navy
B.S., Drexel University, 1999
M.S., Naval Postgraduate School, 2006

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SPACE OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
September 2014

Author: Brian Connett

Approved by: Alex Bordetsky
Thesis Advisor

Daniel W. Bursch
Second Reader

Rudy Panholzer
Chair, Space Systems Academic Group

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Reliance on aging monolithic overhead physical systems with assurance of resilience is an ongoing critical discussion. The White House has issued a strategy to evolve this system of systems technology to meet growing information and knowledge needs.

Fractionated Space Cyber Physical Systems is part of a novel concept emerging from a field of hyperconnected networks designed to withstand risk and address aforementioned needs. The transition from a monolithic design into alternative resilient designs will better reflect the utility of a system to the commander. Resilience is a characteristic meant to assure performance even within a higher probability of risk. Resilience encourages availability regardless of the perceived threat in the increasingly dynamic environment.

Traditional systems incorporate the sub-systems required to deliver the common operational picture. Reduction of those integrated sub-systems is unacceptable; therefore, introducing a decentralized architecture is going to carry with it the requirement of a seamless interaction despite being separated. Decentralization is a design process that allows a constellation capability to seek more nodes than what would be normally available when residing in the same payload. This is a measure of design success that enhances the evaluation of a system's capability and its ability to survive risk, its resilience.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

C5I	Command& Control, Communications, Computers, Combat Systems, and Intelligence
CDHS	Communication & Data Handling Subsystem
CC	Connection Control
COP	common operational picture
CPC	Call Preparation Control
CPS	cyber-physical system
DARPA	Defense Advanced Research Projects Agency
DOD	Department of Defense
DOS	denial of service
DTN	disruption-tolerant network
ECLSS	Environmental Control and Life Support Subsystem
EO	executive order
EPS	Electrical Power Subsystem
F6	Future, Fast, Flexible, Fractionated, Free-flying Spacecraft
GWOT	global war on terrorism
ISR	Intelligence, Surveillance and Reconnaissance
LQE	Linear Quadratic Estimator
LQR	Linear Quadratic Regulator
MANET	mobile ad hoc network
MDTN	Mobile Disruption Tolerant Network
MOP	measures of performance
MTBF	mean time between failures
MTBR	mean time between repairs
NE	network elements
NSSS	National Security Space Strategy
OEF	Operation Enduring Freedom
OIF	Operation Iraqi Freedom
OSI	Open Systems Interconnection
PD	presidential directive
PNT	Position, Navigation and Timing
PS	propulsion subsystem

QoS	quality of service
SCS	Spacecraft Control Subsystem
SBG	Space Based Group
SoS	system of systems

ACKNOWLEDGMENTS

I would like to thank the following individuals for their guidance, support, patience and encouragement:

Dana Connett
Sean Connett
Maile Connett

Professor Alex Bordetsky
Professor Dan Bursch
Professor Steve Tackett

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Current Command, Control, Communications, Computers, Combat Systems and Intelligence (C5I) needs can be more efficiently integrated into U.S. DOD-controlled space-based technology. According to the *NDIA Business and Technology* magazine, and a Satellite Industry Association study after the initial Iraq invasion, "80 percent of all military traffic used during the Iraq invasion traversed many of the 232 commercial satellites orbiting the planet."[1] The failure to create and sustain Intelligence, Surveillance and Reconnaissance (ISR), Position, Navigation and Timing (PNT), communications and strike networks for the sole use by the U.S. military and its allies comes mostly at the risk-adverse strategy of using a monolithic architecture that is commonly thought to be less robust, and even less redundant.

Recently, the Defense Advanced Research Projects Agency (DARPA) noted that "due to lack of satellite over flight opportunities, inability to receive direct satellite downlinks at the tactical level and information flow restrictions … the lowest echelon members of the U.S. military deployed in remote overseas locations are unable to obtain on-demand satellite imagery in a timely and persistent manner for pre-mission planning."[2] In addition to DARPA's claim, hesitancy exists in the form of flexibility, robustness and cyber resiliency concerns. Operation Iraqi Freedom (OIF), Operation Enduring Freedom (OEF) and the global war on terrorism (GWOT) were all victims of the changing fiscal priorities, limiting the funding and fielding of new military satellites. Additionally, asynchronous program cycles continue to make it difficult for the Department of Defense (DOD) to match the resilience and survivability on orbit with terminal deployments, which commercial developers can provide[3]. Specific

[1] John Stanton., "Military to Increase Dependence on Commercial Communications," *National Defense Magazine,* June 2004.

[2] Defense Advanced Research Projects Agency (DARPA), "OnDemand Satellite Imagery Envisioned for Frontline Warfighters," news release, March 12, 2012, http://www.darpa.mil/newsevents/releases/2012/03/12.aspx.

[3] Dustin Kaiser, "Military Communications a Key Target for Satellite Services," *MilsatMagazine*, January 2011.

confidentiality, integrity and availability issues exist beyond the procurement and employment of communications systems. This paper evaluates the resilience of a Space Cyber Physical System and importance of how revaluating space strategy risk acceptance in alternative space architecture can lead to greater availability, reducing the aforementioned hurdles to continued space dominance.

A. MOTIVATION

On June 28, 2010, President Barack Obama announced the administration's New National Space Policy[4] as direction for the nations' space activities. The policy articulated the president's commitment to reinvigorating U.S. leadership in space for the purposes of maintaining space as a stable and productive environment. A key tenet of the policy is that the United States remains committed to the use of space systems in support of its national and homeland security.

"The United States will invest in space situational awareness capabilities […]; develop the means to assure mission essential functions enabled by space; enhance our ability to identify and characterize threats; and deter, defend, and if necessary, defeat efforts to interfere with or attack US or allied space systems."[5] A fiscally and physically constrained strategy encourages retreat from monolithic satellite constellations in exchange for alternative architectures such as space-based groups or fractionated satellites because of the resilience, flexibility, and robustness. This sentiment, according to the National Security Space Strategy (NSSS), avails itself in future investment into space capabilities to include "resilience as a key criterion in evaluating alternative architectures."[6]

Consideration for the need to measure the operability, dependability and cyber resilience of clustered architectures, supporting the growing favorable approach to

---

[4] White House, *The National Space Policy of the United States of America* (Washington, DC: Government Printing Office, June 28, 2010).

[5] Ibid.

[6] Secretary of Defense and Director of National Intelligence, *National Security Space Strategy (NSSS)* (Washington, DC: Secretary of Defense and Director of National Intelligence, January 2011.)

clustered architecture is necessary. In February 2013, an executive order (EO) on cybersecurity along with a presidential directive (PD) on critical infrastructure security and resilience were published to further acknowledge and reinforce the need to "drive action toward a whole community approach to security and resilience."[7] The outward executive support stemming from this EO/PD is not just toward private sector infrastructure supporting the national fervor of eminence, it is also meant to direct efficient situational awareness necessary to incorporate resiliency between military cyber and space physical systems (CPS).

To best evaluate these attributes, dynamic needs and challenges must be examined. In particular, the extent to which the U.S. defense branches and agencies use overhead in support of collection, communications, storage, positioning, navigation, and timing systems and how that can fit into a growing resilient cyber physical system posture needs to be examined. This growing posture can be addressed well by first evaluating resilient communications architecture concepts proposed to support the current command and control environment.

Two particular and tangible concepts exist today that closely align with one another. These concepts are the starting point for the revaluation and give a genesis of a connected cyber physical space system / networked control system: the Space Based Group (SBG) and DARPA's System F6 Program.

The clustered architecture concept first gained momentum at the 2007 AIAA Responsive Space Conference and quickly supported a presentation in the Astrodynamics Specialist Conference and finally with the F6 program start. According to Collopy and Sundberg,[8] the SBG concept "fractionates large, monolithic, multi-mission spacecraft … [and] … dissimilar satellites in compatible orbits, into a group of smaller and simpler

[7] Exec. Order No. 13636 of February 12, 2013, "Improving Critical Infrastructure Cybersecurity," Code of Federal Regulations, title 3 (2013). http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

[8] Paul Collopy and Eric Sundberg, "Creating Value with Space Based Group Architecture" (AIAA 2010-8799), presented at the AIAA Space 2010 Conference & Exposition, Anaheim, CA, Aug. 30–Sept 2, 2010.

utility and single mission spacecraft." This separation of spacecraft capabilities among smaller systems provides continuity throughout the cluster even if other portions of the systems suffer significant delay in communications, a catastrophic failure, a cyber-attack or simply are unavailable for regular preventative maintenance.

This concept of a partitioned, yet effective, operating cyber physical system is closely related to the work of Cramer, Sudhoff and Zivi.[9] They designed performance metrics for systems subject to hostile disruptions, based on the assumption that a system of systems operating in any adverse environment will always have to account for disruption. It is this disruption that returns the scope back to the original premise that the U.S. defense C5I and attack constructs depend largely on continuity of communications and the key ideas of the NSSS. Once the reliability to command and control through technology reaches acceptable probabilities of success, the DOD will be able to completely integrate space into the overall mission.

Finally, like many experts in the field of fractionation, Brown and Eremenko[10] note that while a variety of attributes might "differentiate fractionated architectures from monolithic ones," there remains a value paradigm to be examined; ultimately assigning a measure that "reflects the utility of a particular system to its stakeholder." These attributes differentiate one system from another, Brown and Eremenko continue, and are derived from the value of the underlying mission. Some of the attributes defined by Cramer et al., and Brown and Eremenko will be examined more closely but with the addition of cyber resilience.

B. RESEARCH QUESTIONS

Revaluation of the underlying strategic mission depends on the complete set of derivative value metrics. To that end, the following research questions are identified:

---

[9] Aaron M. Cramer, Scott D. Sudhoff, and Edwin Zivi, "Performance Metrics for Electric Warship Integrated Engineering Plant Battle Damage Response," *IEEE Transactions on Aerospace and Electronic Systems* 47, no, 1, January 2011.

[10] Owen Brown, Paul Eremenko and Paul Collopy. "Value-Centric Design Methodologies for Fractionated Spacecraft: Progress Summary from Phase 1 of the DARPA System F6 Program," (AIAA Paper 2009-6540). Reston, VA: American Institute of Aeronautics and Astronautics, 2009.

- What is space cyber resilience?
- How can fractionation affect resilience?
- How can cyber-resilience be quantified and used as a dynamic network behavior?
- Can a quantifiable resilience follow traditional control theory and data network behaviors?

C. BACKGROUND AND DISCUSSION

Analysis is an evaluation of current and emerging cyber physical systems and the underlying value of the system via military-defined standards of reliability, availability, flexibility, robustness and survivability, tying U.S. space policy and U.S. C5I rules directly to the technologies available. Specifically, the following observations will define the various characteristics and concerns of each "-ility". And, although it is an emerging engineering field, cyber resilience is a formidable measure of performance and measure of success, with significant measuring consideration that will strengthen this discussion.

Taxing requirements on the nodes of CPS of systems exist, which require constant monitoring and decision-making processes regardless of the systems input, outputs and sensed values. Beyond the requirements and physical attributes of a system, it is the constraints of delay and loss that contribute to the instability of a communications system of systems (SoS). With this, reliability and availability will lose its weighted value when measured across a large sample set of data, as suggested by the comparison of the Riemann and Lebesgue[11] sampling processes. As military defined standards, both availability and reliability are appropriate measures of performance (MOP).

Availability is a measure of the degree to which an item is in an operable and committable state at the start of a mission when the mission is called for at an unknown (random) time[12][13]. Reliability is, for non-redundant systems, the duration or probability

[11] Riemann is the normal approach to digital control and to sample periodically in time. Lebesgue is an alternative to Riemann and is normally best described as event based sampling

[12] Department of Defense (DOD), *Definitions of Terms of Reliability and Maintainability* (Washington, DC: Department of Defense, June 1981).

of failure-free performance under stated conditions; and for redundant systems reliability is the probability that an item can perform its intended function for a specified interval under stated conditions[14]. The important distinction within reliability falls to the characteristic of redundancy. To wit, it is important to restrict the scope to measure these characteristics only when the resources provided by the cluster are needed by the mission commanders.

Second, flexibility is determined before the spacecraft leaves the ground and applied when subsequently inserted into its orbit. This weighted MOP is expected to change simply due to the ever-changing technology advances and mission changes that are typically enough to force the need to introduce emerging technologies and techniques while in orbit. With this, a weighted measurement of flexibility turns to envelop the function of its interfacing standards and specifications. When interfacing standards and specifications are open and unambiguous, flexibility will not be the C5I integration deterrent. Further examination, of the OSI models' physical and protocol layers will support that claim and identify the benefit of a targeted study[15].

Flexibility and robustness are explained at length by Brown and Eremenko as the "ultimate source of the enhanced value and reduced risk offered by fractionated architecture." [16] Expansion on these concepts lay the integral foundation on which adding cyber resilience as another "-ility" is certainly the natural progression[17].

Next, survivability, as explained by Cramer et al. and the *Survivability Design Handbook for Surface Ships,*[18] can arguably be the single best design metric for the

---

[13] Item stated at start of a mission includes the combined effects of the readiness-related system parameters but excludes mission time.

[14] DOD, *Definitions of Terms of Reliability and Maintainability*.

[15] Owen Brown and Paul Eremenko, *Application of Value-Centric Design to Space Architectures: The Case of Fractionated Spacecraf*t (AIAA Paper 2008-7869) (Reston, VA: American Institute of Aeronautics and Astronautics, 2008.)

[16] Ibid.

[17] Ibid.

[18] U.S. Navy, *U.S. Navy Survivability Design Handbook For Surface Ships. Chief of Naval Operations Ship Safety and Survivability Office,* OPNAV P-86-4-99, Washington, DC: U.S. Navy, 2000.

inclusion of a complex cyber physical system into the overall C5I construct of the U.S. military. DOD Regulation 5000.2-R is clear that "mission-critical systems … shall be survivable to the threat levels anticipated in their operating environment."[19]

Finally, the resilience of any complex CPS is simply an extension of this existing set of definitions[20]. This set is used to define the need of any complex system to not only survive any adverse action but also to withstand that adverse action while continuing actions necessary to overall mission of that system, a fault tolerant control system. The global community-led initiative, The *Partnership for Cyber Resilience,* launched at the World Economic Forum Annual meeting in 2012 defines cyber resilience as the "ability of systems … to withstand cyber events, measured by the combination of mean time to failure and mean time to recovery [and] can only be achieved by adopting a holistic approach of the management of cyber risk."[21] Still, using only these two parameters to define cyber resilience we find of the four combinations in Table 1, only one outcome gives confidence of a resilient system. That is, when the mean time between failures (MTBF) approaches infinity, and the mean time to repair (MTTR) approaches zero, only then is a system truly resilient. There must be more parameters that define the resilience of any complex system, therefore, providing the user greater confidence when valuing the cyber resilience of the system.

[19] "Mandatory Procedures for Major Defense Acquisition Programs," DOD Regulation 5000.2R, Washington, DC: Department of Defense, April 5, 2002.

[20] It is of utmost importance to highlight at this junction that while cost, an identified attribute to optimization, is a crucial decision criterion, but not considered here.

[21] World Economic Forum (WEF), *Risk and Responsibility in a Hyperconnected World Pathways to Global Cyber Resilience* (New York: World Economic Forum, June 2012).

↓cyber resilience	↑MTBF	↑MTTR
↑cyber resilience	↑MTBF	↓MTTR
↓cyber resilience	↓MTBF	↑MTTR
↓cyber resilience	↓MTBF	↓MTTR

Table 1. Cyber Resilient Combinations

In a 2011 DOD fact sheet addressing the *Resilience of Space Capabilities,* [22] several key ideas underpinning resilience are listed. Primarily related to this analysis, the fact sheet states the purpose of resilience is to "assure performance of military and related intelligence functions at a level necessary to execute assigned mission within an acceptable tolerance for risk." Language consistency exists among mission assurance professionals and through the DOD definition that the mission functions and mission successes are critical parameters to the overall architecture resilience. This resiliency, therefore, increases as the system can be made available at a greater rate of usage and time regardless of the perceived or actual threat of adverse actions.

Experience alone tells us that the difference between mitigating risk and completely avoiding failure is a daunting task. However, there are guiding principles of precedence that empower the engineering process to specifically consider the dangers of a low-resilient CPS. These dangers can be evaluated with a common occurring analysis criteria found in the 2011 DOD *Resilience of Space Capabilities* document. When measuring the systems performance, resilience is most critical when measuring the time during which a mission commander is waiting for the services of the constellation to restore its services[23]. Nonetheless, the criteria through which space cyber physical design

[22] "Resilience of Space Capabilities," Department of Defense, accessed September 19, 2014. http://www.defense.gov/home/features/2011/0111_nsss/docs/DoD%20Fact%20Sheet%20-%20Resilience.pdf.

[23] Ibid.

and institutionalization can occur while being quantified exists in the NSSS, especially when the "domain is increasingly congested, contested and competitive"[24]:

1. Anticipated level of adversity
2. Functional capability goals necessary to support the mission
3. The risk that these goals may not be met at a given level of adversity
4. The severity of the functional shortfall to the mission
5. The time that the shortfall can be tolerated by the mission

[24] Ibid.

THIS PAGE INTENTIONALLY LEFT BLANK

II. SPACE CYBER PHYSICAL SYSTEMS

A. WHAT IS A CYBER PHYSICAL SYSTEM?

A cyber physical system is the successful and continuous "integration of computation with physical processes, which involve communication, computation, sensing, and actuating through heterogeneous and widely distributed physical devices and computation components"[25]. This synergy depends heavily on a resilient infrastructure that can provide near-continuous communications connections that are capable of behaving within operational standards regardless of the inputs and sensor determinations. Most recently, and by extension, this space-based cyber physical system of systems is easily defined in the framework of the Internet of Things (IOT), or Industry 2.0. In the *Global Information Technology Report 2012*, the World Economic Forum reports "hyperconnected communications includes not only people-to-people formats, but also communication between people and machines, and between machines themselves without any direct human involvement."[26] This is both the promise and peril of hyper connectivity for organizations and societies as we depend more on the hyperconnected internet of sensors, actuators and plants, which, in turn, is depending more on the autonomous satellite system in order to provide global control of devices connected to each other.

Traditional definitions of CPS stop short of explaining the integration of control. Two in the emerging field, do not; rather in their perspective of CPS, Kim and Kumar refer to the "next generation engineered systems that require tight integration of computing, communication, and control technologies to achieve stability, performance, reliability, robustness, and efficiency in dealing with physical systems of many

[25] Lichen Zheng, "Multi-view Approach to Specify and Model Aerospace Cyber-physical Systems," presented at the IEEE 16th International Conference on Computational Science and Engineering, Sydney, Australia, 3-5 December 2013.

[26] "The Global Information Technology Report 2014 Rewards and Risks of Big Data," World Economic Forum, 2014.

application domains." [27] Originally called a field of hybrid-systems, it soon shifted its field name to cyber-physical systems to encapsulate the natural interface of physical, computing and communications pieces. As the societal calls multiplied for ever-increasing connectivity between devices, soon sensing elements were desired to understand the physical environment in which the CPS existed. This new addition, sensing, connected alongside the actuators and controllers of the closed loop system allowed realization of a truly networked CPS. These engineered systems rely heavily upon the integration of control and computational components with physical processes. Figure 1 illustrates an example simple design of a modern CPS/NCS and illustrates that CPS encompass more than just critical infrastructure.

As the developed overhead satellite SoS progresses with advanced computing and communications technologies, the overall human dependence on a resilient CPS will increase. Normally, the physical systems are designed to protect it when it senses abnormalities along the communications nodes, exactly the goal of a space cyber-physical fractionated architecture. Now, architecture is designed to reduce the monolithic footprint and volume of the physical overhead portion, while enhancing and hyper connecting the cyber portion of the ever-growing information and communication technologies.

[27] Kyoung-Dae Kim and P.R. Kumar, "Cyber-Physical Systems: A Perspective at the Centennial," *Proceedings of the IEEE* 100, (May 2012): 1287.

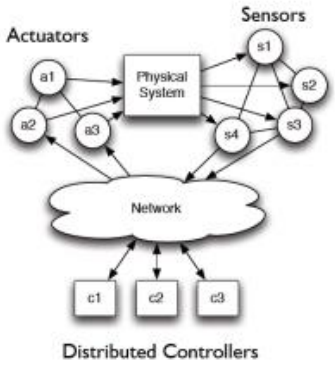

Figure 1. General Architecture of a CPS[28]

B. CPS AND CYBER RESILIENCY CHALLENGES

There are countless reasons for which to dedicate any effort in making a space CPS resilient and risk averse. The World Economic Forum offered a framework in 2012 to further the dialogue of CPS challenges, in Figure 2:

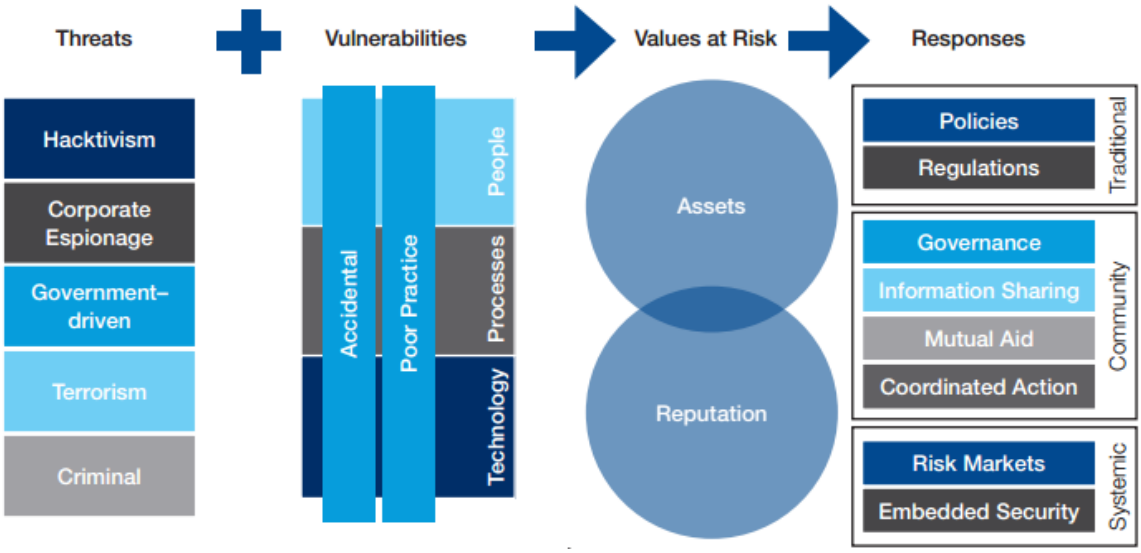

Figure 2. Cyber Risk Framework[29]

[28]Alvaro A Cardenas, Saurabh Amin and Shankar Sastry, "Secure Control: Towards Survivable Cyber-Physical Systems," paper presented at the 28th International Conference on Distributed Computing Systems Workshops, Berkeley, CA, June 2008.

Four distinct areas, identified in Figure 2, are used to create a dialogue toward a standard of global understanding while hyper connectivity of the growing amount of devices becomes immeasurable. The framework laid out is useful for this evaluation to explain the reason that fractionated or SBG CPS architecture is an optimal approach to ensure resiliency.

The first of the distinct areas, Threats, are used to identify stable controller approaches to isolate the present and future threats, and associated risk. This is a fundamental step regardless of physical or policy design. Second, the vulnerabilities addressed in the WEF report enveloped the discussion in that vulnerability exists only from an "accidental" or "poor practice" stand point; whereas any vulnerability to an emerging technology such as the SBG might simply emerge from the speed with which access-skillsets mature. [30] Overhead satellites CPS do not have the advantage of continued physical access in order to modify the assigned payload, ensuring evolving and fortifying security. The aggregate of threats and vulnerabilities produces *values at risk* in order to address the assets and reputation of the system. Most important in this context, and more validating to the point that fractionated satellite systems are a key to resilient systems, is that assets include the "integrity, availability, and security of data, networks and connected devices." [31]These subjective values of the assets are seemingly addressable when discussing a specific networked method by which to provide a greater level of resilience in a fractionated CPS.

Finally, responses that are traditional, cooperative and systemic will often result in a system being largely non-resilient. Instead (in the same sense that assuring an asset is fortified, available and secure), system success falls to a resilient response. The methods of payload management and the manner in which the CPS sensors respond with the environment "provide additional insight into operations," according to Cutler, Atkins and

---

[29] WEF, *Risk and Responsibility in a Hyperconnected World*.

[30] Ibid.

[31] Ibid.

Klesh.[32] This is an observation critical to responses and awareness for payload collaboration; especially in a fractionated environment.

[32]James W. Cutler, Ella M. Atkins, Andrew T. Klesh, "Cyber-Physical Challenges for Space Systems," paper presented at the IEEE/ACM Third International Conference on Cyber-Physical Systems, Beijing, China, April 17–19 2012.

THIS PAGE INTENTIONALLY LEFT BLANK

III. MOTIVATIONAL EXAMPLE: FRACTIONATION AND SPACE-BASED GROUP CYBER PHYSICAL SYSTEM

A. INTRODUCTION

The Defense Advanced Research Projects Agency, an organization whose initial existence came to be based on great investment has made many unintended successful stories of high-risk. The Tactical Technology Office has an objective to "transform the future of war fighting through high risk, high payoff development of rapid, mobile, and responsive combat performance for advanced weapons, platforms, and space systems."[33] This details the advances to space systems that DARPA wants in order to provide resilience, assured access and stability.

B. FRACTIONATION ARCHITECTURE

Traditionally, a monolithic single-mission spacecraft is built around a payload and supported by the various subsystems required to execute those missions, to include the spacecraft control subsystem (SCS), communication and data handling subsystem (CDHS), electrical power subsystem (EPS), environmental control and life support subsystem (ECLSS), and propulsion subsystems (PS).[34] In the comparison depicted in Figure 3, Mathieu and Weigel illustrate "an equivalent fractionated spacecraft that consists of the same components but are physically separated into a payload module and one or several infrastructure modules."[35]

---

[33] "Mission Objectives," Defense Advanced Research Projects Agency, accessed September 23, 2014, http://www.darpa.mil/Our_Work/TTO.

[34] Jerry Sellers et al., *Understanding Space: An Introduction to Astronautics* (New York: Learning Solutions, 2007).

[35] Charlotte Mathieu and Annalisa Weigel, "Assessing the Fractionated Spacecraft Concept," (AIAA Paper 2006-7212) (Reston, VA: American Institute of Aeronautics and Astronautics, 2006.)

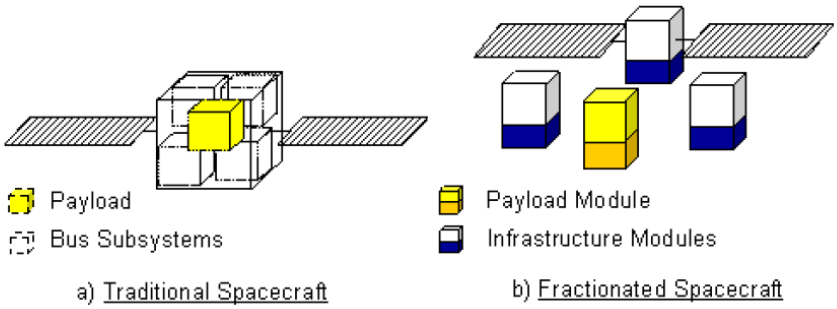

Figure 3. Traditional versus Fractionated Spacecraft[36]

By comparison, the DARPA F6 (Future Fast, Flexible, Fractionated, Free-Flying Spacecraft) is the actual realization of a fractionated concept originally awarded simultaneously to four of the aerospace industry giants to demonstrate resilience. The word resilience is not used as metric; rather it is the combination of the key definitions assigned in the mission requirements, namely flexibility and robustness. As is depicted in Figure 3, the fractionated concept derives its success largely from the idea of a decentralized missions payload methodology. The decentralized method allows continued operation of physically separated modules regardless of the environment or mission status. This characteristic can be strengthened further and made to be more resilient if consideration is given to applying fault-control or estimation controls to prevent erroneous or malicious data from enter the fractionated mission system. The F6 program, displayed in Figure 4, illustrates that the distributed life, cluster and payload systems are a consideration in the fractionated architecture, but more prevalent is the overlapping capabilities of networking, wireless communications, power transfer and distributed computing.

[36] Ibid.

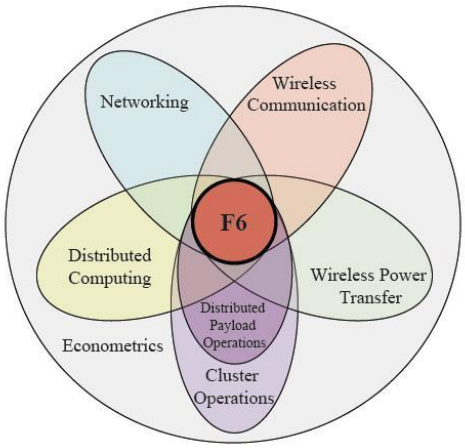

Figure 4. F6 Program Capability Overlaps[37]

A mobile ad hoc network (MANET) and overcoming a hidden terminal problem, clearly are within the idea of a decentralized architecture like the fractionated system, and can still remain resilient when combined with classical control theories such as consensus control, Kalman filtering or a linear quadratic regulation techniques in order to provide optimal control over the data. Even still, with an ad hoc network there remains the need to maintain the end-to-end connectivity because the ability to distinguish between network control information and actual message data cannot be separated in such a design.

C. HOW CAN FRACTIONATION AFFECT RESILIENCE?

Tolerance for risk, and the ability to execute an assigned mission, according to the 2011 Space Systems report to the DOD, is what best defines the quality of a resilient system.[38]. There are physical and non-physical components of the fractionated architecture, which lend best to this posture, but if observation of two specific layers of the Open Systems Interconnection (OSI) conceptual model is used, another dynamic emerges to support resilient fractionation knowledge integrity. Layers 2 and 3 of OSI

[37] "System F6," Defense Advanced Research Projects Agency, accessed September 23, 2014, http://www.darpa.mil/Our_Work/TTO/Programs/System_F6.aspx.

[38] "Resilience of Space Capabilities", Department of Defense, accessed September 19, 2014, /DoD%20Fact%20Sheet%20-%20Resilience.pdf.

model (Data Link and Network) are protocols on which estimation and data assurance are critical to the resilience of the fractionated space segment. Layer 2, the data link layer provides a line to the third layer that is seemingly free of transmission errors. Layer 3 will then route those packets from the source to some destination. Here in the third layer there are numerous functions susceptible to control denial such as modulating, demodulating, addressing, and protocol deconfliction. These are two layers that are often subject to the attack and denial of service (DOS), which ultimately renders the system useless because the information flowing across cannot be trusted.

Fractionation of the satellite capabilities across many modular pieces could provide the ideal architecture for allocating the required intelligent agents and less expensive network elements to which, according to Bordetsky, "provides a unique testbed for identifying and assessing risks of operating technically advanced orbital systems for managing mission critical multipoint collaborative tasks."[39] Bordetsky's conversation focuses largely on using software agents collaboratively with real-time applications that require optimal management of information and bandwidth, without disruption or delay. When normally housed in the same payload or bus, the integrity of layers is susceptible to chaotic failure.

Two layers of feedback control, Call Preparation Control and Connection Control, introduce adaptive control among the bandwidth usage[40] but now as a fractionated system to support resilience of data continuity. Call Preparation Control is an important aspect of the fractionation design, in that it allows for seamless connection based on previous sessions but it is not essential to the confidentiality, integrity or availability of the current session. Assurance of the data in the current short-term communications session across fractionated modules is derived from the Connection Control requirements, which is summarized in the Bordetsky paper of celestial networks:

- Supervising provided Quality of Service (QoS) parameters

[39] Alex Bordetsky, "Celestial Data Routing Network," in *Proceedings of SPIE: Vol. 4136. Small Payloads in Space*, eds. Brian J. Horais and Robert J. Twiggs (Bellingham,WA: SPIE, November 2000).

[40] Ibid.

- Providing flow control, congestion control, routing, reservation and renegotiation of resources
- Modifying and releasing connections[41]

The Connection Control algorithms and supporting decision criteria do not address the integrity of the information, rather the criteria is largely concerned with the availability of the information. While a system can assure availability by maintaining the connection, the fractionated SoS can fall to the fragility of the data, if that data integrity is compromised and allowed to permeate into the system. The process of Connection Control does resemble Bayesian control algorithms and decisions, and appears to be receptive to added parameters of consensus control beyond a decision to apply or surrender bandwidth control. The change, then, to the Connection Control is extending the amount of time a communication or decision module will retain its previous communication packet before releasing it, in a system that can be inherently stable, such as a well-defined satellite communications orbit. Passing data that are stored for a finite amount of time is becoming less prohibitive as storage solutions become more robust and less expensive, leaving this option of connection control over time still viable.

Another approach to consider is that of a Disruption-Tolerant Network (DTN), which is designed into SoS that are heterogeneous by design in order to successfully execute its given mission. Both protocols and systems that support the delivery protocol-dependent information are found in this heterogeneity but often encounter incompatibility. The significant fault that is apparent in traditional networking design is the desire for the algorithm of a network to seek out an end-to-end transmission path of communication before actually delivering its information. Seeking this flawless communication path in a challenged environment can decrease the MTBF rendering the system non-resilient. A DTN is suitable for fractionated systems with networks experiencing unpredictable connections, and therefore absent an end-to end connection.

[41] Ibid.

The combination of Connection Control and Disruption-Tolerant Networking techniques establishes the foundation on which a protocol can successfully and confidently pass information and knowledge along a fractionated space CPS. These two techniques establish a history of trusted communications links along a lengthened time line by the nature of holding packets longer before making routing decisions. Still, when a decision is made to route specific network traffic and its content on the payload there is no guarantee that the system remains resilient. There remains a final fractionated hardening technique that strengthens the validity of the payload.

A fractionated communications network is a unique setup in a space-based architecture. A fractionated system is best understood as a mobile ad hoc network (MANET) that can be characterized by intermittent connectivity for a variety of reasons, such as atmospheric effects, system availability and electromagnetic interference. Intermittent connectivity can also become an issue, and not readily apparent, if the information passes between fractionations and satisfies the connection and protocol controls. This intermittent connectivity may be a hostile attack against the CPS, in any combination of three methods of encroachment.

A mobile ad hoc network is clearly within the idea of a decentralized architecture like the fractionated system, and can still remain resilient when combined with classical control theories such as consensus control, Kalman filtering or a linear quadratic regulation techniques in order to provide optimal control over the data. Even still, with an ad hoc network there remains the need to maintain the end-to-end connectivity because the ability to distinguish between network control information and actual message data cannot be separated in such a design. A favorable assumption about the nodes in a MANET architecture is that they are treated independently. This is consistent with the approach toward a fractionated system in order to "guarantee the communication between the sender node and receiver node"[42]regardless of hopping protocol or module failures.

[42] A.H. Azni, Rabiah Ahmad, and Zul Azri, "Resilience and Survivability in MANET: Discipline, Issue and Challenge," paper presented at the 3rd International Conference on Computing and Informatics, Bandung, Indonesia, June 2011.

D. SPACE CYBER PHYSICAL SYSTEM VULNERABILITIES

According to Cardenas et al., there are three styles of hostile attack: deception, denial of service, and a direct attack against the physical fractionation[43].

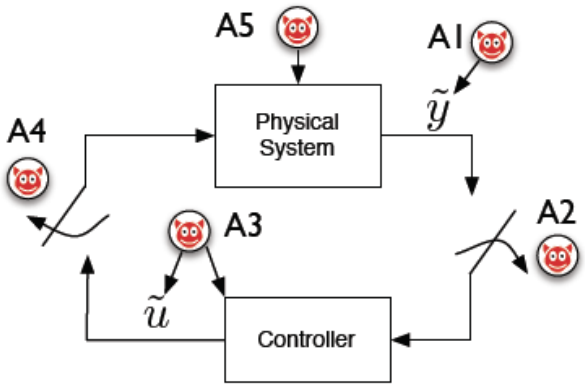

Figure 5. CPS Vulnerabilities[44]

Deception attack (Figure 5: injection point A1 or A3) is the misuse of real information or use of misinformation, through the use of a compromised communication link key, sensor or controller. The attacker in a denial of service (Figure 5: A2 or A4) prevents the physical system from receiving a control signal, or prevents the controller from receiving sensor data. The third deception attack (Figure 5: A5) is a direct attack against the modules and its specific physical equipment. The three of these deception attacks can be countered, mitigated and nullified if a distributed estimation across the information network is placed. The distribution of the information over many fractionated modules seeking some final value can eliminate any ambiguity as to the originality of the data and information penetrating the CPS.

---

[43] Alvaro A Cardenas, Saurabh Amin and Shankar Sastry. "Secure Control: Towards Survivable Cyber-Physical Systems," paper presented at the 28th International Conference on Distributed Computing Systems Workshops, Berkeley, CA, June 8-9,2008.

[44] Ibid.

By fractionating a space cyber physical system of systems or networked architecture, it becomes a feasible problem to address the connection control, default tolerance and consensus control simultaneously. Addressing in this manner with a strict definition of the goals of a resilient control and a measure of the SoS robustness, we start to see the value fractionation gives to resilience.

E. HOW CAN CYBER-RESILIENCE A BE QUANTIFIED AND USED AS A DESIGN METRIC?

While discussing the architecture and its values at risk, and then again during the resilience of a fractionated system, attention was briefly given to estimation and tolerance filters to determine the value (real, safe, complete) of the data crossing between each module. This value is a direct correlation to the amount of resilience the systems can be said to exhibit. Each of the fractionated overlapping capabilities of data, communication or energy transfer areas of operations are ones which seemingly follow the fundamental precept of an estimation filter like Kalman, which produces estimates of current variables and its associated uncertainties, then compares those to the next piece of information to formulate a weighted/moving estimation of the integrity of the data. Closely aligned to this estimation concept is a store and forward (Figure 6) methodology employed by mobile disruption tolerant network (MDTN) protocols between physical systems nodes. In fractionation, resilience is further assured when the communications of the method are still possible despite a seemingly absent receiver node due to the described vulnerabilities.

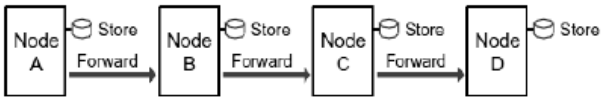

Figure 6. DTN Store and Forward Concept[45]

[45] Claudio E Palazzi, Marco Roccetti, Armir Bujari, Stefano Bonetta, Gustavo Marfia "MDTN: Mobile Delay/Disruption Tolerant Network," paper presented at the 20th International Conference on Computer Communications and Networks, Maui, Hawaii, July 31–August 4, 2011.

Disruption tolerance processes can help define the metrics by which cyber-resilience can be measured in a fractionated architecture. Palazzi et al. describe successful DTN interconnecting communications nodes that "accommodate the mobility and limited power evolving wireless communication devices."[46] A major tenet of labeling a system resilient has been its availability, a metric that can be weakened when characterized by typical wireless behaviors such as intermittent connectivity, delays due to error or physical inaccessibility. In the MDTN discussion by Palazzi et al., the store and forward message concept strengthens resilience of the system by maintaining the actual reliable information crossing nodes despite the vulnerabilities present. In order to conceptually map fractionated communications architecture, it is incredibly convenient to review the motivation of a DTN in order to address the assurance of confidentiality, integrity, and availability in a fractionated system, but in terms of the fractionation valuation[47]:

1. Spacecraft subsystem availability lends greater opportunity to maintain broken communications
2. Fractionated subsystems offer multiple nodes through which communications can be maintained
3. Error checking measures can be employed across multiple modules assigned to the constellation
4. Retransmission of information, or rerouting of information simultaneously across decentralized architecture offers integrity

Because the store and forward method of a mobile network waits with information for best opportunity to transmit, a fractionated and decentralized system offers greater fidelity by creating more moments of transmission.

[46] Ibid.

[47] Ibid.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. CONCLUSION

Current U.S. DOD command and control posture closely correlates to the valuation placed on the space strategy risk valuation designed and implemented with great adversity in mind. Alternative space architectures and constellation can lead to greater confidence in a system of system capable of transmitting healthy information, increasing the overall value of the space cyber physical systems being employed. Despite the space strategy and apparent desire to move forward that is supported by executive orders and presidential directives, there still remains requirements to apply due diligence in assuring that the information delivered to the commander is good. The discussion of the piece focused largely on defining or reviewing the characteristics necessary to drive the value of a fractionated system.

Space Cyber Physical Systems of Systems and fractionated architectures are poised to deliver the strategic position of space dominance, or terrestrial dominance from space. The transition from a monolithic design into such alternative designs will better reflect the utility of a system to the commander in the form of the military standard characteristics of availability, flexibility, robustness, survivability, and resiliency. The most latter is a characteristic meant to assure performance even within a range of higher probability of risk. This resilience assurance also encourages availability regardless of the perceived threat in the increasingly dynamic environment.

Providing near-continuous hyper-connectivity among the heterogeneous system of systems is a desired vision that is permeating most mission sets available today. This has been a growing expectation by users, but the risk associated with the reliability of information has also grown. The ability to control the way information is used cannot rely on the algorithmic information technologies methodologies. There must now be a reliance on control methodologies capable of inching towards sufficient self-awareness. Still, there are challenges and complexities with any effort to become autonomous and safe. This can be modeled in a cyber systems risk framework built upon the aggregate of a systems threats and vulnerabilities. When those two are understood and combined to create the most complete risk picture, we can then start to place values on the risk and

develop what the responses can be … a conclusion to being sufficiently self-aware and capable of providing the real-time continuous connections.

The examples used to demonstrate the decentralized architectures required to be hyper-connected were the space-based group and fractionated systems currently being examined in several industries, including space operations. As described several times, the traditional monolithic systems incorporate the necessary sub-systems required to deliver the most common operational picture (COP) to the commander. Any reduction or removal of those integrated sub-systems is not acceptable, therefore introducing a decentralized architecture is going to carry with it the requirement of a seamless interaction despite being separated in space. The decentralization is a physical engineering design process that allows a constellation capability to seek more nodes of connectivity than what would be normally available when residing in the same payload. This is a measure of design and design success which enhances the weighted valuation of a system's capability and its ability to survive risk; its resilience.

When combined with classical control methods, physical decentralization and algorithmic mobile ad hoc networking allows a system to maintain its end-to-end connectivity. This fractionation is direct effect on resilience of the overall system by focusing on physical separation but also on the technological allocation of intelligent agents and real-time application capable of producing a sufficiently aware system. Methods of connection and preparation control assure that the information that is being sent across any of the nodes is actually the healthy information not affected by the threat in the environment. Combined with the suitable approach of disruption tolerance foundations are further strengthened allowing the confident transmission of the information and knowledge along the network. With physical and virtual preparation, transmission and controls procedures in place we next sought to understand the CPS vulnerabilities present in the environment. As described by many researchers, the styles of hostile attack are significant enough to render a system helpless, and even sometimes irrecoverable.

Finally, measuring and quantifying cyber resilience to be used as a design metric was examined in closing, but should be the starting point for future research for space cyber physical systems.

THIS PAGE INTENTIONALLY LEFT BLANK

V. FUTURE RESEARCH

Measuring and quantifying cyber resilience is starting point for future research for space cyber physical systems. Through estimation, tolerance filters and self-awareness a systems value can be designed accurately to give the greatest value, in that is real data, safe data, and complete data. When maximized, it is possible that the valuable data is directly correlated to a highly resilient system. The methodology by which one can ensure that a datum is valuable is through active and decisive control across nodes. A process in the mobile disruption tolerant network, the store and forward method should be a focus of research and simulation to verify a resilient network despite an environment with seemingly absent receiver nodes due to the various hostile or physical disruptions discussed.

Developing disruption tolerances and acceptable risk levels in order to accommodate limitations of power and data is a major tenet of declaring a system resilient. The actual availability and reliability of information, regardless of hostilities, is a measurement that should be examined and integrated if proven effective. Ultimately, this quantified value can extend the conceptual mapping of known DTN architectures, as discussed in Palazzi et al., [48]to those fractionated architectures processes. In applying the boundaries from which the metrics can be derived, an orthogonal array (Table 2) aligned tightly to the conceptual map provided in the aforementioned discussion lays out a possible orthogonal array experiment from which a researcher can begin to assign resilience value to its observed SoS.

	LOCAL SUBSYSTEMS	FRACTIONATED SUBSYSTEMS	ERROR CHECKING	REROUTING/RETRANSMISSION
LOCAL SUBSYSTEMS				
FRACTIONATED SUBSYSTEMS				
ERROR CHECKING				
REROUTING/RETRANSMISSION				

Table 2. Orthogonal Array Example–Resilience

[48] Ibid.

THIS PAGE INTENTIONALLY LEFT BLANK

BIBLIOGRAPHY

Astrom, Karl Johan, and Bo Bernhardsson. "Comparison of Riemann and Lebesgue Sampling for First Order Stochastic Systems." In *Proceedings of the 41st IEEE Conference on Decision and Control*, Piscataway, NJ: IEEE, Dec. 10–13, 2002. doi: 10.1109/CDC.2002.1184824

Azni, A.H., Rabiah Ahmad, and Zul Azri. "Resilience and Survivability in MANET: Discipline, Issue and Challenge." In *Proceedings of the 3rd International Conference on Computing and Informatics*, Bandung, Indonesia: ICOCI, June 8-9, 2011.

Bilbao-Osorio, Beñat Soumitra Dutta, and Bruno Lanvin, eds. *The Global Information Technology Report 2014: Rewards and Risks of Big Data*. Geneva: World Economic Forum, 2014.

Bordetsky, Alex, "Celestial Data Routing Network." In *Proceedings of SPIE, Small Payloads in Space Vol. 4136*, edited by Brian J. Horais and Robert J. Twiggs, Bellingham, WA: SPIE, November 2000. doi:10.1117/12.406647.

Brown, Kendall K. *Space Power Integration: Perspectives from Space Weapons Officers* Maxwell Air Force Base, AL: Air University Press, 2006.

Brown, Owen, and Paul Eremenko. *Application of Value-Centric Design to Space Architectures: The Case of Fractionated Spacecraf*t (AIAA Paper 2008-7869). Reston, VA: American Institute of Aeronautics and Astronautics, 2008.

Brown, Owen, and Paul Eremenko. *The Value Proposition for Fractionated Space Architecture*s (AIAA Paper 2006-7506). Reston, VA: American Institute of Aeronautics and Astronautics, 2006.

Brown, Owen, Paul Eremenko, and Christopher Roberts. *Cost-Benefit Analysis of a Notional Fractionated SATCOM Architecture* (AIAA Paper 2006-5328). Reston, VA: American Institute of Aeronautics and Astronautics, 2006.

Brown, Owen, Paul Eremenko, and Paul Collopy. *Value-Centric Design Methodologies for Fractionated Spacecraft: Progress Summary from Phase 1 of the DARPA System F6 Program* (AIAA Paper 2009-6540). Reston, VA: American Institute of Aeronautics and Astronautics, 2009.

Brulle, Robert V. *Engineering the Space Age: A Rocket Scientist Remembers.* Maxwell Air Force Base, Ala.: Air University Press, December 2008.

Cardenas, Alvaro A., Saurabh Amin, and Shankar Sastry. "Secure Control: Towards Survivable Cyber-Physical Systems." (IEEE Computer Society Paper 1545-0678/08). Paper presented at The 28th International Conference on Distributed Computing Systems Workshops, Beijing, China, June 2008.

Clark, Vern. "Sea Power 21: Projecting Decisive Joint Capabilities." *Proceedings Magazine (United States Naval Institute),* 2002.

Collopy, Paul, and Eric Sundberg. "Creating Value with Space Based Group Architecture," (AIAA 2010-8799). Paper presented at the AIAA Space 2010 Conference & Exposition, Anaheim, CA, Aug. 30–Sept. 2, 2010.

Cramer, Aaron M, Scott D. Sudhoff, and Edwin Zivi. "Performance Metrics for Electric Warship Integrated Engineering Plant Battle Damage Response." *IEEE Transactions on Aerospace and Electronic Systems* 47, no. 1 (January 2011).

Cutler, James, W., Ella M. Atkins, and Andrew T. Klesh. "Cyber-Physical Challenges for Space Systems," Paper presented at the 2012 IEEE/ACM Third International Conference on Cyber-Physical Systems, Beijing, China, April 2012.

Defense Advanced Research Projects Agency (DARPA). "OnDemand Satellite Imagery Envisioned for Frontline Warfighters," March 12, 2012.

Department of Defense. *Military Standard. Definitions of Terms of Reliability and Maintainability* (MIL-STD-721C). Washington, DC: Department of Defense, June 1981.

Kim, Kyoung-Dae, and P.R. Kumar. "Cyber-Physical Systems: A Perspective at the Centennial," *Proceedings of the IEEE, Special Centennial Issue,* May 13, 2012.

Lambeth, Benjamin S. *Mastering the Ultimate High Ground, Next Steps in the Military Uses of Space*. Santa Monica, CA: RAND, 2006.

Mathieu, Charlotte, and Annalisa Weigel. *Assessing the Fractionated Spacecraft Concept* (AIAA Paper 2006-7212). Reston, VA: American Institute of Aeronautics and Astronautics, 2006.

National Research Council. *The Navy's Needs in Space for Providing Future Capabilities.* Washington, DC: The National Academies Press, 2005.

Palazzi, Claudio E., Marco Roccetti, Armir Bujari, Stefano Bonetta, and Gustavo Marfia. "MDTN: Mobile Delay/Disruption Tolerant Network." Paper presented at the 20th International Conference on Computer Communications and Networks, Maui, Hawaii, 2011.

Richards, Matthew, Daniel Hastings, Donna Rhodes, and Annalisa Weigel. "Defining Survivability for Engineering Systems." Paper presented at 2007 Conference on Systems Engineering Research, Hoboken, NJ, March 14–16, 2007.

Sellers, Jerry J. *Understanding Space: An Introduction to Astronautics*. New York: McGraw Hill, 2004), 368–374.

Stanton, John. "Military to Increase Dependence on Commercial Communications," *National Defense Magazine,* June 2004.

Stehr, Mark-Oliver, and Carolyn Talcott. "Planning and Learning Algorithms for Routing in Disruption-Tolerant Networks." IEEE *Military Communications Conference 2008* 1, no. 8 (November 2008): 16–19, doi: 10.1109/MILCOM.2008.4753336.

U.S. Joint Chiefs of Staff. *Joint Doctrine for Space Operations* (JP 3-14), Washington, DC: U.S. Joint Chiefs of Staff, 2009.

U.S. Department of Defense. *DoD Executive Agent for Space.* DOD Directive 5101.2. Washington, DC: U.S. Department of Defense, 2003.

U.S. Department of Defense. *Mandatory Procedures for Major Defense Acquisition Programs.* DOD Regulation 5000.2R. Washington, DC: U.S. Department of Defense, 2002.

U.S. Department of Defense. "Resilience of Space Capabilities." Accessed September 19, 2014. http://www.defense.gov/home/features/2011/0111_nsss/docs/DoD%20Fact%20Sheet%20-%20Resilience.pdf

U.S. Navy, (CNO-SSSO). *US Navy Survivability Design Handbook For Surface Ships*, OPNAV P-86-4-99, Washington, DC: U.S. Navy (CNO-SSSO), 2000.

Wertz, James R. and Wiley J Larson, *Space Mission Analysis and Design*. Torrance, CA: Microcosm, 1999.

White House. *The National Space Policy of the United States of America*. Washington, D.C.: Government Printing Office, June 28, 2010.

World Economic Forum. "Risk and Responsibility in a Hyperconnected World Pathways to Global Cyber Resilience." June 2012. http://www.weforum.org/reports/risk-and-responsibility-hyperconnected-world-pathways-global-cyber-resilience

Zhang, Lichen, "Multi-view Approach to Specify and Model Aerospace Cyber-physical Systems." Paper presented at the 2013 IEEE 16th International Conference on Computational Science and Engineering, Dec 2013. Doi: 10.1109/CSE.2013.94

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California